FortiAnalyzer

Security Analysis Report

Report Date: 2013-10-19

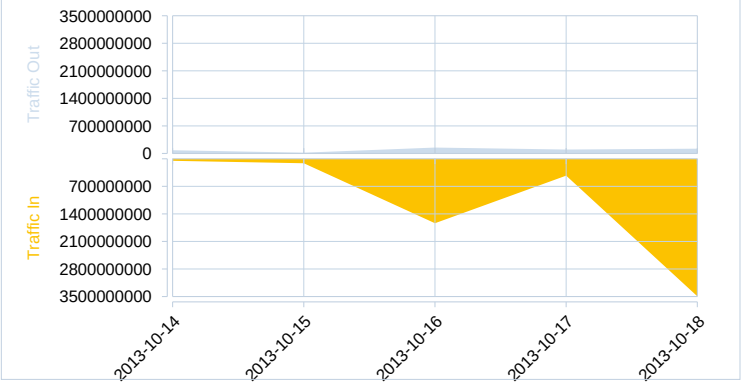
Data Range: 2013-10-12 00:00 - 2013-10-18 23:59 CEST (FAZ local)

FORTINET

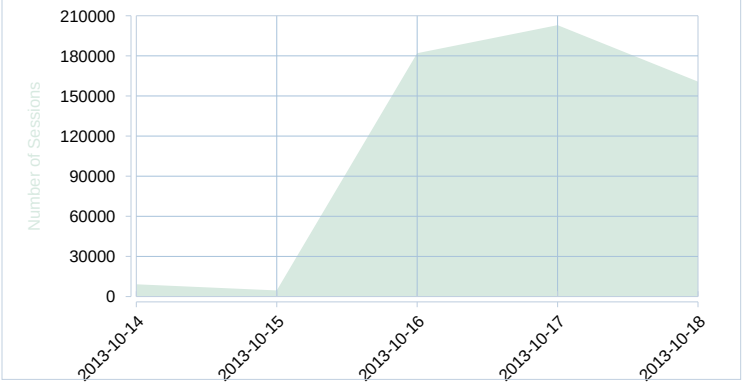
Table of Contents

Bandwidth and Applications

Traffic Bandwidth for Past 7 days



Number of Sessions for Past 7 days



Top Users by Bandwidth

User	IP	Bandwidth	Traffic Out	Traffic In
198.18.3.2	198.18.3.2			4.22 GB
198.18.0.1	198.18.0.1			408.20 MB
198.18.0.17	198.18.0.17			361.84 MB
217.193.240.162	217.193.240.162			332.60 MB
198.18.1.11	198.18.1.11			128.97 MB
198.18.0.18	198.18.0.18			105.38 MB
195.65.5.169	195.65.5.169			46.03 MB
solivaan	195.65.5.169			27.98 MB
184.178.47.136	184.178.47.136			23.70 MB
198.18.3.5	198.18.3.5			23.25 MB

Top Users by Sessions

User	IP	Sessions
198.18.0.18	198.18.0.18	11938
173.199.69.203	173.199.69.203	11858
184.178.47.136	184.178.47.136	11370
72.20.56.150	72.20.56.150	8695
207.161.128.38	207.161.128.38	7994
12.181.120.130	12.181.120.130	7815
198.18.0.11	198.18.0.11	7705
77.233.249.180	77.233.249.180	7618
198.18.1.11	198.18.1.11	7489
78.70.73.94	78.70.73.94	7324

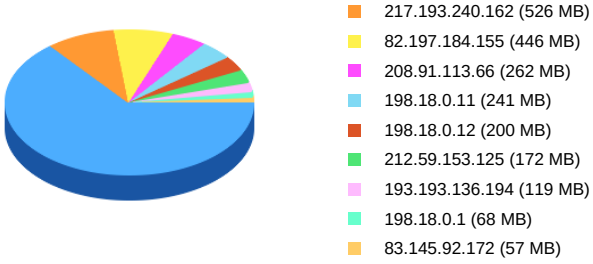
Top Applications by Bandwidth

Application	Bandwidth	Traffic Out	Traffic In
Domain Name Server			779.90 MB
514/tcp			197.51 MB
541/tcp			173.02 MB
Web Management(HTTPS)			66.02 MB
SSLVPN			47.12 MB
HTTPS			34.47 MB
gNTP			26.27 MB
ESP.UDP			23.57 MB
IMAPS			5.08 MB
Web Management			2.20 MB

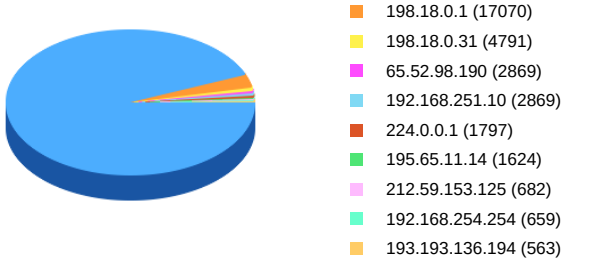
Top Applications by Sessions

Application	Sessions
Domain Name Server	523436
8612/udp	4547
47963/udp	1201
gNTP	1084
17500/udp	1073
Web Management(HTTPS)	896
137/udp	841
Skype	717
138/udp	556
8620/udp	507

Top Destination Addresses by Bandwidth



Top Destination Addresses by Sessions



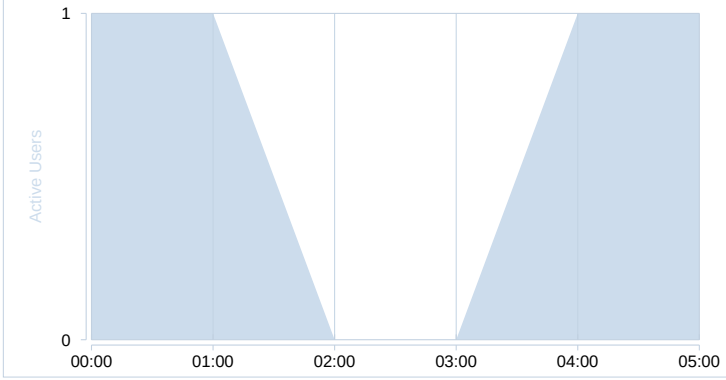
DHCP Summary

Interface	Allocated IP (%)	New Clients Count
port2.FG300C3913601712	14.29	6
port2.FG300C3913602452	14.29	6

Top Wifi Client by Bandwidth

No matching log data for this report

Traffic History by Number of Active Users



Web Usage

Top Web Users by Blocked Requests

User (or IP)	Hostname (or Mac)	Requests
198.18.0.18	wsmacpro2	281
198.18.1.11		31
198.18.0.17		3
198.18.3.5		2
198.18.0.17	e8:40:f2:89:7b:a1	1
198.18.3.4		1

Top Web Users by Allowed Requests

User (or IP)	Hostname (or Mac)	Requests
198.18.1.11		1.27 K
198.18.3.2		367
198.18.0.18	wsmacpro2	310
198.18.0.17	SatellitePro770	241
198.18.3.5		99
198.18.0.17		81
198.18.0.13	00:0c:29:bc:42:66	55
198.18.3.4		48
198.18.0.17	e8:40:f2:89:7b:a1	36
198.18.0.12	00:0c:29:36:5c:0f	8

Top Web Users by Bandwidth

User	IP	Bandwidth	Traffic Out	Traffic In
198.18.3.2	198.18.3.2	4.21 GB		
198.18.0.17	198.18.0.17	70.39 MB		
198.18.1.11	198.18.1.11	47.21 MB		
198.18.0.18	198.18.0.18	11.63 MB		
198.18.3.4	198.18.3.4	6.65 MB		
198.18.3.5	198.18.3.5	2.99 MB		
198.18.0.11	198.18.0.11	2.57 MB		
198.18.0.12	198.18.0.12	2.56 MB		
198.18.0.13	198.18.0.13	386.54 KB		

Top Web Users by Browsing Time

User	Browsing Time(Mins)	Sent	Received
198.18.1.11	438.80		128.97 MB
198.18.0.17	238.57		361.84 MB
198.18.0.18	150.70		105.38 MB
198.18.3.2	53.50		4.22 GB
198.18.3.4	15.05		11.19 MB
198.18.3.5	8.13		23.25 MB
198.18.0.13	5.05		662.71 KB
198.18.3.7	3.28		406.24 KB
198.18.0.14	2.00		3.19 MB

Top Web Users by Bandwidth (contd)

User	IP	Bandwidth	Traffic Out	Traffic In
198.18.0.14	198.18.0.14	15.20 KB		

Top Web Users by Browsing Time (contd)

User	Browsing Time(Mins)	Sent	Received
198.18.0.11	1.53		6.54 MB

Top Blocked Websites by Requests

Website	Requests
notify10.dropbox.com	168
ui.skype.com	107
46.165.192.221	31
r8---sn-nfpnnjvh-9anl.c.pack.google.com	4
www.sex.com	3
www.eicar.org	1
www.classicshell.net	1
versioncheck.busymac.com	1

Top Allowed Websites by Requests

Website	Requests
tools.cisco.com	107
news-tags.cisco.com	105
www.cisco.com	98
safebrowsing.clients.google.com	90
safebrowsing-cache.google.com	79
tools-tags.cisco.com	61
partners-tags.cisco.com	61
h20566.www2.hp.com	59
www.fortiguard.com	55
cisco-tags.cisco.com	52

Top Allowed Web Sites by Bandwidth

Website	Bandwidth	Traffic Out	Traffic In
h30537.www3.hp.com	3.29 GB		
vsphereclient.vmware.com	762.20 MB		
fg.v4.download.windowsupdate.com	68.83 MB		
sdlc-esd.sun.com	67.28 MB		
download.oracle.com	32.11 MB		
support.netapp.com	16.73 MB		
208.91.113.73	12.56 MB		
www.cisco.com	8.82 MB		
personal.avira-update.com	8.35 MB		
ftp.hp.com	7.81 MB		

Top Web Domains by Browsing Time

Domains	Browsing Time(Hrs)	Sent	Received
safebrowsing.clients.	2.54		229.42 KB
37.252.254.6	2.15		3.33 MB
notify10.dropbox.com	1.72		750.44 KB
crl.microsoft.com	1.35		110.20 KB
safebrowsing-cache.	1.10		7.13 MB
ds.download.window	0.64		81.47 KB
sales.liveperson.net	0.38		2.13 MB
217.146.21.5	0.27		46.94 KB
rps-svcs.sun.com	0.26		2.50 KB
www.google.ch	0.26		283.52 KB

Emails

Top Senders by Number of Emails

Sender	Number of Emails
198.18.0.18	8
82.165.146.105	2
146.0.73.121	2
66.195.207.213	1
113.200.250.26	1
218.59.209.140	1
212.92.98.18	1

Top Senders by Combined Email Size

Sender	Combined Email Size
198.18.0.18	35.98 KB

Top Recipients by Number of Emails

Recipient	Number of Emails
198.18.0.18	48
84.52.64.125	8
198.18.3.4	4
74.208.184.231	1

Top Recipients by Combined Email Size

Recipient	Combined Email Size
198.18.0.18	6.76 MB
198.18.3.4	102.52 KB

Threats

Top Viruses by Name

Virus Name	Occurrences
EICAR_TEST_FILE	2

Top Virus Victims

Virus Victims	Occurrences
198.18.0.17	2

Top Attack Sources

No matching log data for this report

Threats

Top Attack Victims

No matching log data for this report

VPN Usage

Top Site-to-Site IPSec Tunnels by Bandwidth

No matching log data for this report

Top Dial-Up IPSec Tunnels by Bandwidth

No matching log data for this report

Top SSL-VPN Tunnel Users by Bandwidth

User	IP	Bandwidth	Traffic Out	Traffic In
solivaan				24.10 MB
roospi				6.34 MB

Top SSL-VPN Web Mode Users by Bandwidth

User	IP	Bandwidth	Traffic Out	Traffic In
solivaan				24.10 MB
roospi				6.34 MB

Top Dial-Up VPN Users

User	Type	Aggregated Dialed Time	Aggregated Bytes
solivaan	ssl-web	27m 56s	24.10 MB
roospi	ssl-web	12m 25s	6.34 MB
campbja	ssl-web	5m 46s	0

VPN Traffic Usage Trend

No matching log data for this report

Admin Login and System Events

Admin Login Summary

Date/Time	User Name	Login Interface	Duration	Config Change	Device
10/18 05:10	admin		1m 27s	✓	alsochlu-sg0e2
10/18 05:10	admin		49s	✗	alsochlu-sg0e2
10/18 05:10	admin		25s	✗	alsochlu-sg0e2
10/18 04:10	admin		52s	✗	alsochlu-sg0e2
10/18 04:10	admin		25m 17s	✓	alsochlu-sg0e2
10/18 02:10	admin		12m 54s	✓	alsochlu-sg0e2
10/18 01:10	admin		21m 56s	✓	alsochlu-sg0e2
10/18 12:10	admin		3m 35s	✓	alsochlu-sg0e2
10/18 12:10	admin		14m 13s	✓	alsochlu-sg0e2
10/18 12:10	admin		15m 9s	✓	alsochlu-sg0e2
10/17 07:10	admin		23m 39s	✗	alsochlu-sg0e1
10/17 07:10	admin		8m 1s	✓	alsochlu-sg0e1
10/17 06:10	admin		45m 47s	✓	alsochlu-sg0e1
10/17 02:10	admin		15m 46s	✓	alsochlu-sg0e2

Date/Time	User Name	Login Interface	Duration	Config Change	Device
10/17 01:10	admin		6m 37s	✓	alsochlu-sg0e1
10/17 01:10	FMG-Admin-al		1m 30s	✗	alsochlu-sg0e2
10/17 01:10	FMG-Admin-al		1m 53s	✓	alsochlu-sg0e2
10/17 01:10	FMG-Admin-al		25s	✗	alsochlu-sg0e1
10/16 08:10	admin		1m 5s	✗	alsochlu-sg0e1
10/16 08:10	admin		34m 43s	✓	alsochlu-sg0e1
10/16 05:10	admin		15m 25s	✗	alsochlu-sg0e1
10/16 04:10	admin		15m 50s	✗	alsochlu-sg0e1
10/16 04:10	FMG-Admin-al		4m 13s	✓	alsochlu-sg0e1
10/15 08:10	admin		21m 12s	✗	alsochlu-sg0e1
10/15 08:10	admin		42m 41s	✓	alsochlu-sg0e1
10/15 07:10	admin		25m 4s	✓	alsochlu-sg0e1
10/15 06:10	admin		1m 52s	✓	alsochlu-sg0e1

System Active Summary

Date/Time	Events	Device
10/18 02:10	DHCP statistics	alsochlu-sg0e1
10/18 02:10	DHCP statistics	alsochlu-sg0e2
10/18 01:10	DHCP statistics	alsochlu-sg0e2
10/18 01:10	DHCP statistics	alsochlu-sg0e1
10/18 12:10	DHCP statistics	alsochlu-sg0e1
10/18 12:10	DHCP statistics	alsochlu-sg0e2
10/18 11:10	DHCP statistics	alsochlu-sg0e1
10/18 11:10	DHCP statistics	alsochlu-sg0e2
10/18 10:10	DHCP statistics	alsochlu-sg0e1
10/18 10:10	DHCP statistics	alsochlu-sg0e2
10/18 09:10	DHCP statistics	alsochlu-sg0e1
10/18 09:10	DHCP statistics	alsochlu-sg0e2
10/18 08:10	DHCP statistics	alsochlu-sg0e1
10/18 08:10	DHCP statistics	alsochlu-sg0e2
10/18 08:10	The ntp daemon step adjusted time from Fri Oct 18 17:24:	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-cisco:	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-hp:5	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-ibm:5	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-root:5	alsochlu-sg0e2
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-cisco:	alsochlu-sg0e1
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-hp:5	alsochlu-sg0e1
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-ibm:5	alsochlu-sg0e1
10/18 08:10	Delete vpn.ssl.web.portal:widget full-access-VDOM-root:5	alsochlu-sg0e1
10/18 08:10	Assigns IP address/configuration parameters to the client	alsochlu-sg0e2
10/18 08:10	Client requests IP address/configuration parameters	alsochlu-sg0e2
10/18 07:10	DHCP statistics	alsochlu-sg0e1
10/18 07:10	DHCP statistics	alsochlu-sg0e2
10/18 07:10	Completed reputation db maintenance	alsochlu-sg0e1
10/18 07:10	Completed reputation db maintenance	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2

Date/Time	Events	Device
10/18 07:10	SSL tunnel shutdown	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2

System Active Summary (contd)

Date/Time	Events	Device
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL alerts	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user:widget:bookmarks roospi gr-SSL-V	alsochlu-sg0e1
10/18 07:10	Add vpn.ssl.web.user:widget roospi gr-SSL-VPN-VDOM-r	alsochlu-sg0e1
10/18 07:10	Add vpn.ssl.web.user roospi gr-SSL-VPN-VDOM-root	alsochlu-sg0e1
10/18 07:10	Add vpn.ssl.web.user:widget:bookmarks roospi gr-SSL-V	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user:widget roospi gr-SSL-VPN-VDOM-r	alsochlu-sg0e2
10/18 07:10	Add vpn.ssl.web.user roospi gr-SSL-VPN-VDOM-root	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2

Date/Time	Events	Device
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL web application closed	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL web application activated	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2
10/18 07:10	SSL new connection	alsochlu-sg0e2

Appendix A - Individual Report for 1st Highest Bandwidth User: 198.18.3.2 Usage: 4 GB IP: 198.18.3.2 Device: N/A

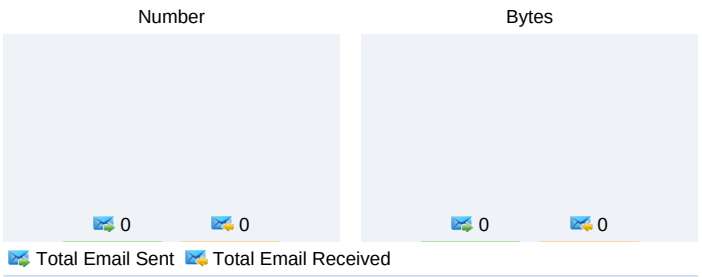
Traffic Summary

Total Number of Sessions	1.4 K	
Total Number of Bytes	4.2 GB	
	4.1 GB in	76.1 MB out

Top 5 Destinations

Destination	Number of Sessions	App
198.18.0.1	610	Domain Name Server
15.216.76.82	139	
15.217.232.251	62	
82.197.184.154	37	
216.245.17.109	28	

Email Activity Summary



Top 5 Email Recipients

Recipient	Bandwidth

Top 5 Email Senders

Sender	Bandwidth

Web Activity Summary

Top 10 Allowed Sites

Site Name	Number of Sessions
h20566.www2.hp.com	59
fg.v4.download.windowsupdate.com	28
ocsp.verisign.com	18
h18004.www1.hp.com	16
welcome.hp-ww.com	14
www.also.ch	11
ctldl.windowsupdate.com	10
java.com	10
clients1.google.com	10
www.hp.com	9

Top 10 Blocked Sites

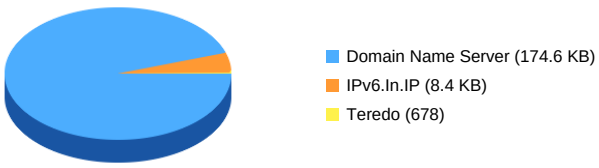
Site Name	Number of Sessions

Threat Summary

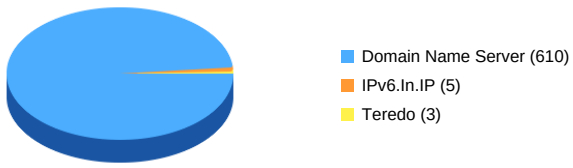
Threat Name	Type	Counts
EICAR_TEST_FILE		2

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Appendix B - Individual Report for 2nd Highest Bandwidth User: 198.18.0.1 Usage: 408 MB IP: 198.18.0.1 Device: N/A

Traffic Summary

Total Number of Sessions	637
Total Number of Bytes	408.2 MB
	218.6 MB in / 189.6 MB out

Top 5 Destinations

Destination	Number of Sessions	App
198.18.0.12	297	514/tcp
198.18.0.11	151	Web Management(HTTPS)
198.18.0.11	106	541/tcp
198.18.0.1	30	Web Management(HTTPS)
198.18.0.14	24	1812/udp

Email Activity Summary

Number		Bytes	
0	0	0	0

Total Email Sent | Total Email Received

Top 5 Email Recipients

Recipient	Bandwidth

Top 5 Email Senders

Sender	Bandwidth

Web Activity Summary

Top 10 Allowed Sites

Site Name	Number of Sessions

Top 10 Blocked Sites

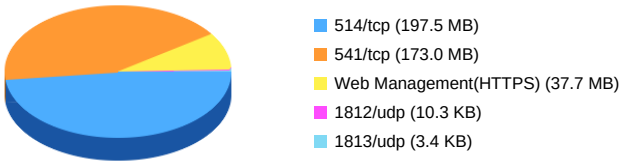
Site Name	Number of Sessions

Threat Summary

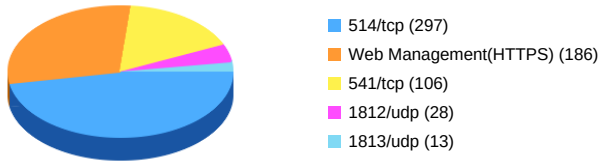
Threat Name	Type	Counts
EICAR_TEST_FILE		2

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Appendix C - Individual Report for 3rd Highest Bandwidth User: 198.18.0.17 Usage: 332 MB IP: 198.18.0.17 Device: Satellite

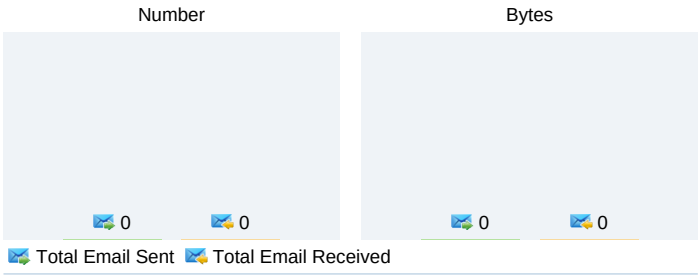
Traffic Summary

Total Number of Sessions	1.6 K
Total Number of Bytes	331.9 MB
	322.8 MB in / 9.1 MB out

Top 5 Destinations

Destination	Number of Sessions	App
198.18.0.1	710	Web Management(HTTPS)
198.18.0.31	709	137/udp
198.18.0.1	573	Domain Name Server
198.18.0.31	464	138/udp
208.91.113.73	49	

Email Activity Summary



Top 5 Email Recipients

Recipient	Bandwidth

Top 5 Email Senders

Sender	Bandwidth

Web Activity Summary

Top 10 Allowed Sites

Site Name	Number of Sessions
safebrowsing.clients.google.com	55
safebrowsing-cache.google.com	47
208.91.113.73	46
javadl.sun.com	14
www.fortinet.com	12
ocsp.verisign.com	10
www.oracle.com	8
ds.download.windowsupdate.com	7
gtssl-ocsp.geotrust.com	7
mscrl.microsoft.com	7

Top 10 Blocked Sites

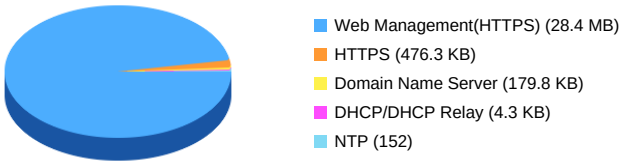
Site Name	Number of Sessions
www.sex.com	3
www.eicar.org	1

Threat Summary

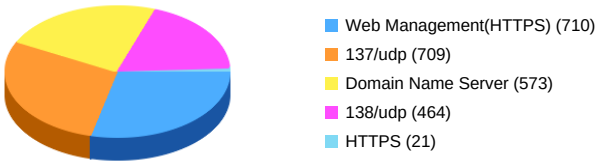
Threat Name	Type	Counts
EICAR_TEST_FILE		2

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Appendix D - Individual Report for 4th Highest Bandwidth User: 217.193.240.162 Usage: 333 MB IP: 217.193.240.162 Device

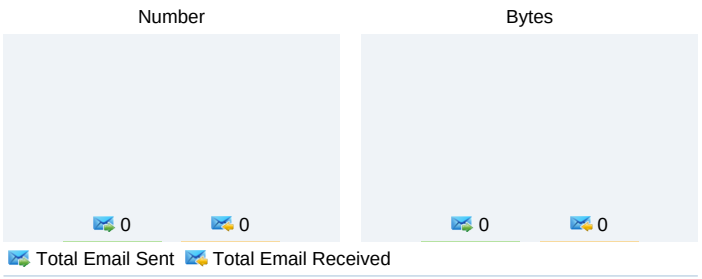
Traffic Summary

Total Number of Sessions	1.8 K
Total Number of Bytes	332.6 MB
	311.7 MB in / 20.9 MB out

Top 5 Destinations

Destination	Number of Sessions	App
212.59.153.125	682	Domain Name Server
193.193.136.194	563	Domain Name Server
208.91.112.220	233	Domain Name Server
91.240.0.5	30	gNTP
208.91.113.184	28	HTTPS

Email Activity Summary



Top 5 Email Recipients

Recipient	Bandwidth

Top 5 Email Senders

Sender	Bandwidth

Web Activity Summary

Top 10 Allowed Sites

Site Name	Number of Sessions

Top 10 Blocked Sites

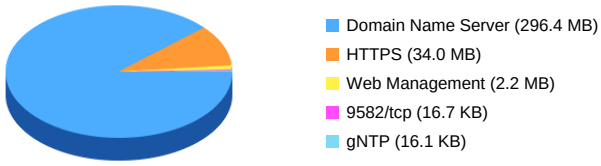
Site Name	Number of Sessions

Threat Summary

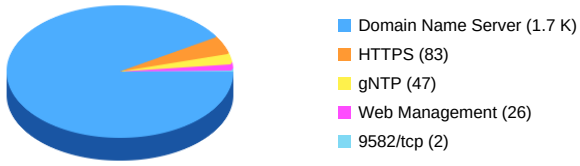
Threat Name	Type	Counts
EICAR_TEST_FILE		2

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Appendix E - Individual Report for 5th Highest Bandwidth User: 198.18.1.11 Usage: 129 MB IP: 198.18.1.11 Device: N/A

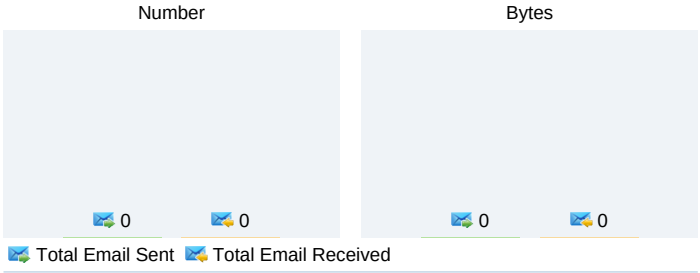
Traffic Summary

Total Number of Sessions	7.5 K
Total Number of Bytes	129.0 MB
	100.2 MB in / 28.7 MB out

Top 5 Destinations

Destination	Number of Sessions	App
65.52.98.190	2.9 K	
198.18.0.1	2.2 K	Domain Name Server
157.56.149.250	251	
72.163.10.14	107	
2.23.96.170	106	

Email Activity Summary



Top 5 Email Recipients

Recipient	Bandwidth

Top 5 Email Senders

Sender	Bandwidth

Web Activity Summary

Top 10 Allowed Sites

Site Name	Number of Sessions
tools.cisco.com	107
news-tags.cisco.com	105
www.cisco.com	98
partners-tags.cisco.com	61
tools-tags.cisco.com	61
cisco-tags.cisco.com	52
www.microsoft.com	43
crl.microsoft.com	38
sso.cisco.com	35
clients1.google.com	32

Top 10 Blocked Sites

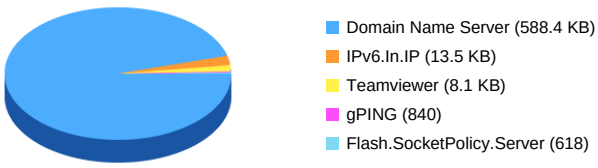
Site Name	Number of Sessions
46.165.192.221	31

Threat Summary

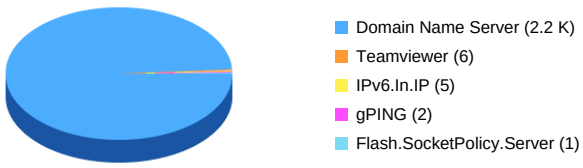
Threat Name	Type	Counts
EICAR_TEST_FILE		2

Application Summary

Top 5 Application Bandwidth



Top 5 Application Sessions



Appendix F

Devices: alsochlu-sg0e0-root